AO 106 (REV 4/10) Affidavit for Search Warrant

AUSA Shawn McCarthy, (312) 353-8881

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNDER SEAL

In the Matter of the Search of:

Case No. 23 M 175

The Apple Inc. account aminbetuni@icloud.com, further described in Attachment A

APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT

I, Daniel Nugent, a Special Agent of the Homeland Security Investigations, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

See Attachment A

located in the Northern District of California, there is now concealed:

See Attachment A, Part III

The basis for the search under Fed. R. Crim. P. 41(c) is evidence and instrumentalities.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, United States Code, Section 554, Title 50, United States Code, Section 4819 and Title 18, United States Code, Section 922(o)	Smuggling Goods From the United States Violations of Export Control Reform Act and Possession of a Machinegun

The application is based on these facts:

See Attached Affidavit,

Continued on the attached sheet.

Applicant's Signature

DANIEL NUGENT, Special Agent
Homeland Security Investigations
Printed name and title

Pursuant to Fed. R. Crim. P. 4.1, this Application is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the statements in the Application and Affidavit by telephone.

Date: February 21, 2023

Judge's signature

City and State: Chicago, Illinois

GABRIEL A. FUENTES, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I, Daniel Nugent, being duly sworn, state as follows:

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"), and have been so employed for approximately fourteen years. Prior to my employment with HSI, I served as a United States Customs and Border Protection ("CBP") Officer from approximately 2003 through 2008.

2. I am currently assigned to the Office of the Special Agent in Charge, Chicago, Illinois, where I conduct investigations relating to violations of federal laws relating to the illegal export of commodities, information, and services from the United States, including Title 13, United States Code, Section 305; Title 18, United States Code, Section 554; and Title 50, United States Code, Section 4819. I am familiar with the federal laws relating to the unlawful export of firearms and other commodities from the United States as specified and regulated by the U.S. Department of State, Directorate of Defense Trade Controls ("DDTC"); the U.S. Department of Commerce, Bureau of Industry and Security ("BIS"); and the U.S. Department of the Treasury, Office of Foreign Assets Controls ("OFAC"). In conducting these investigations, I have used a variety of investigative techniques and resources, including, but not limited to, search warrants, visual surveillance,

electronic surveillance, and the debriefing of defendants, witnesses, informants, and others who have knowledge of violations of federal law. I have participated in numerous investigations involving violations of firearms laws and smuggling laws.

a. This affidavit is made in support of an application for a warrant to search, pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), for information associated with certain account(s) that are stored at the premises owned, maintained, controlled, or operated by Apple Inc. that accepts service at One Apple Park Way, Cupertino, CA 95014; and for information associated with certain accounts that are stored at the premises owned, maintained, controlled, or operated by Google LLC, a free web-based electronic mail service provider located at 1600 Amphitheatre Parkway, Mountain View, California, 94043; and for information associated with certain account(s) that are stored at the premises owned, maintained, controlled, or operated by Microsoft Corporation, a free web-based electronic mail service provider located at One Microsoft Way, Redmond, WA 98052-6399 (the "**Service Providers**"). The accounts to be searched are Apple Inc. account aminbetuni@icloud.com ("**Subject Apple Account 1**"); Google accounts aminbetuni@gmail.com ("**Subject Google Account 1**"), johnny2133@gmail.com ("**Subject Google Account 2**"); and Microsoft account aminbetuni@hotmail.com ("**Subject Microsoft Account 1**") (collectively the "**Subject Accounts**") which are further described in the following paragraphs and in Part II of Attachments A, A-1 and A-2. As set forth below, there is probable cause to believe that in the accounts,

described in Part II of Attachment A, in the possession of Apple Inc., Google LLC, and Microsoft Corporation, there exists evidence and instrumentalities of smuggling goods from the United States in violation of Title 18, United States Code, Section 554, Violations of Export Control Reform Act pursuant to Title 50, United States Code, Section 4819 and possession of a machinegun in violation of Title 18, United States Code, Section 922(o) ("the **Subject Offenses**").

3. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence and instrumentalities of smuggling goods from the United States in violation of Title 18, United States Code, Section 554, Violations of Export Control Reform Act pursuant to Title 50, United States Code, Section 4819 and possession of a machinegun in violation of Title 18, United States Code, Section 922(o), are located in the **Subject Accounts**.

I. BACKGROUND INFORMATION

A. Apple Inc.

4. Based on my training and experience and information available from Apple Inc.'s website (apple.com), I have learned the following about Apple Inc.:

a. Apple is a United States company that produces the iPhone, iPad, iPod Touch, and Apple Watch, which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

b. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

c. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

d. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

e. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

f. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from

Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

g. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

h. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

i. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

j. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies,

and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

k. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

l. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

m. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's

website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

n. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

o. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs

in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

p. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on

iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

5. Based upon the information provided in this affidavit, as well as my training, experience, and the investigation conducted to date, there is probable cause to believe that **Subject Apple Account 1** contains evidence, fruits, and instrumentalities of the **Subject Offenses**. Further, because the primary target and other conspirators unknown to the government have used Apple AirTags and email accounts to smuggle goods from the United States, I believe there is probable cause that email messages, text messages, and other documents stored in **Subject Apple Account 1** are likely to contain evidence of these violations.

6. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

7. The stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are

often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

8. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the offenses under investigation.

9. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

10. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

B. Google LLC

11. Based on my training and experience and information available from Google's website (google.com), I have learned the following information about Google and Gmail:

a. Google offers a collection of Internet-based services, including e-mail and online data storage, which is owned and controlled by Google. The services are available at no cost to Internet users, though there are certain options, such as additional online data storage, that users may elect to pay money to receive. Subscribers obtain an account by registering on the Internet with Google and providing Google with basic information, including name, gender, zip code, and other personal/biographical information. Subscribers are given a Google account which ends in "@gmail.com" which is utilized to access these online services.

b. Google maintains electronic records pertaining to the individuals and entities who maintain Google online subscriber accounts. These records often

include account access information, e-mail transaction information, account application information, and in some circumstances billing and payment information.

c. Any e-mail that is sent to a Google online account subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by Google. If the message is not deleted by the subscriber, the account is below the maximum storage limit, and the subscriber accesses the account periodically, that message can remain on Google's servers indefinitely.

d. When a subscriber sends an e-mail, it is initiated by the user, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google online account users have the option of saving a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Google server, the e-mail may remain on the system indefinitely.

e. Google online account subscribers can store files, including but not limited to e-mails, documents, and image files, on servers maintained and/or owned by Google. The online data storage service is known as "Google Drive."

f. Google online account subscribers can also utilize a feature known as "History" that allows a user to track various historical account activity, including past Google Internet searches performed, information regarding devices which have been used to login to the Google online account, and physical location information regarding from where the Google online account was accessed.

g. Google Maps allows users to search for places and routes to navigate there using public transportation, vehicle, bicycle, or foot. Users can label or designate specific places in Google such as home or work. Google Maps also records commute routes and commute settings based on recorded patterns such as date and time, origin and destination, and route traveled. Google Maps Timeline stores places visited and routes taken based on the user's Location History.

h. Google keeps records that can reveal accounts accessed from the same electronic device, such as the same computer or mobile phone, including accounts that are linked by "cookies," which are small pieces of text sent to the user's Internet browser when visiting websites.

12. Therefore, the computers of Google are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Google, such as account access information, transaction information, and account application.

C. Microsoft Corporation

13. Based on my training and experience and information available from Microsoft's email websites (hotmail.com, outlook.com, live.com), I have learned the following about Microsoft's email services:

a. Microsoft provides email services, including hotmail.com, outlook.com, and live.com. Come, which are available to Internet users. Subscribers obtain an account by registering with the relevant Microsoft email services on its website (*e.g.*, hotmail.com, outlook.com, live.com). Microsoft requests subscribers to

provide basic information, such as name, gender, zip code and other personal/biographical information.

b. Microsoft maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records often include account access information, email transaction information, and account application information.

c. Any email that is sent to a subscriber is stored in the subscriber's "mail box" on Microsoft servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by Microsoft. If the message is not deleted by the subscriber, the account is below the maximum storage limit, and the subscriber accesses the account periodically, that message can remain on Microsoft's servers indefinitely;

d. When the subscriber sends an email, it is initiated by the user, transferred via the Internet to Microsoft 's servers, and then transmitted to its end destination. Microsoft's users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the Microsoft server, the email can remain on the system indefinitely;

e. A Microsoft email subscriber can store files, including emails and image files, on servers maintained and/or owned by Microsoft.

14. Therefore, the computers of Microsoft are likely to contain all the material just described, including stored electronic communications and information

concerning subscribers and their use of Yahoo!, such as account access information, transaction information, and account application.

15. In order to accomplish the objective of the search warrant with minimal interference to the business activities of the **Service Providers**, to protect the rights of the subjects of the investigation, and to effectively pursue this investigation, authority is sought to allow the **Service Providers** to make a digital copy of the entire contents of the information subject to search specified in Section II of Attachment A. That copy will be provided to me or to any authorized federal agent. The contents will then be analyzed to identify records and information subject to seizure pursuant to Section III of Attachment A.

16. The United States, including Homeland Security Investigations (HSI) and the Department of Commerce (DOC), Office of Export Enforcement (OEE), are conducting a criminal investigation of Amin BETUNI regarding possible violations of Title 18, United States Code, Section 554, Title 50, United States Code, Section 4819 and Title 18 United States Code, Section 922(o) ("the **Subject Offenses**").

17. Title 18, United States Code, Section 554(a), makes it a federal crime to fraudulently or knowingly export or send from the United States, or attempt to export or send from the United States, any merchandise, article, or object contrary to any law or regulation of the United States, or receive, conceal, buy, sell, or in any manner facilitate the transportation, concealment, or sale of such merchandise, article, or

object, prior to exportation, knowing the same to be intended for exportation contrary to any law or regulation of the United States.

18. The Export Control Reform Act of 2018 ("ECRA"), 50 U.S.C. §§ 4801-4852, provides for the control of the export, re-export, and in-country transfer of items, and specific activities of United States persons, wherever located, that implicate national security. To that end, ECRA grants the President the authority to control "(1) the export, re-export, and in-country transfer of items subject to the jurisdiction of the United States, whether by United States persons or by foreign persons; and (2) the activities of United States persons, wherever located, relating to" specific categories of items. 50 U.S.C. § 4812. ECRA further grants the Secretary of Commerce the authority to establish the applicable regulatory framework. It is unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under ECRA. 50 U.S.C. §4819. Willful violations of ECRA are crimes punishable by a prison term of up to 20 years and a fine of up to $1,000,000.00. 50 U.S.C. § 4819(b).

19. Pursuant to ECRA's authority, the United States Department of Commerce ("U.S. Department of Commerce" or "DOC") reviews and controls the export of certain items, including commodities, software, and technology, from the United States to foreign countries through the Export Administration Regulations ("EAR"), 15 C.F.R. §§ 730-774. In particular, the EAR restricts the export of items that could make a significant contribution to the military potential of other nations

or that could be detrimental to the foreign policy or national security of the United States. The EAR imposes licensing and other requirements for items subject to the EAR lawfully to be exported from the United States. "Export" is defined in the EAR as an "actual shipment or transmission out of the United States." 15 C.F.R. § 734.13(a)(1).

20. The most sensitive items subject to EAR controls are identified on the Commerce Control List ("CCL"). 15 C.F.R. part 774, Supp. No. 1. Items on the CCL are categorized by Export Control Classification Number ("ECCN") based on their technical characteristics. Each ECCN has export control requirements depending on destination, end user, and end use.

21. The following items are firearms and ammunition which are controlled under ECCN 0A501 and cannot be exported from the United States without a license or written approval from the United States Government: 7.5 inch rifle barrels and gas blocks for a 5.56 rifle.

II. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH

A. Summary

22. Law enforcement has intercepted three packages containing household items with secreted rifle parts. Two of the three packages had a return address to Amin BETUNI at his residence. As described below, BETUNI did not have a license to ship any of the rifle parts overseas.

23. **Subject Google Accounts 1** and **2** as well as **Subject Microsoft Account 1** were used to purchase firearms parts from online gun supply companies

and the firearm parts were shipped to Amin BETUNI's residence. Many of the firearm parts were like firearms parts that BETUNI previously shipped overseas. Several of the shipments contained Apple AirTags, one of which was paired with **Subject Apple Account 1**.

B. AMIN BETUNI

24. According to records maintained by the Cook County Assessor's Office, Amin BETUNI is the owner of 10346 S 73rd Avenue, Palos Hills, Illinois 60465 (the "Subject Premises"). Further, according to the Illinois Secretary of State, Amin BETUNI is the president of Nephews Towing & Recovery Inc. According to Department of Transportation records, the Subject Premises is listed as the business address along with telephone number (708) 275-4569 ("Subject Phone 1").

25. According to Verizon records, as of October 14, 2015, Subject Phone 1 has been subscribed to Amin BETUNI and was subscribed to Subject Premises at the time of the execution of a search warrant on December 21, 2022.

26. According to Illinois State Police records, BETUNI has an active Firearms Owner Identification (FOID) card, as well as a concealed carry permit that are both registered at the Subject Premises.

27. According to Apple records, **Subject Apple Account 1** was created on or about April 16, 2012, is associated with Amin BETUNI, Subject Premises, Subject Phone 1, and has a recovery address of **Subject Microsoft Account 1**.

28. According to Google records, **Subject Google Account 1** was created on or about July 27, 2012, is associated with Amin BETUNI, Subject Phone 1, and has a recovery address of **Subject Apple Account 1**.

C. SUBJECT ACCOUNTS and ONLINE FIREARMS PURCHASES

29. According to Online Gun Supply Company 3, on or about October 26, 2022, BETUNI, using **Subject Microsoft Account 1**, purchased two 7.5 inch AR-15, 5.56 caliber rifle barrels as well as two Glock 19, 9mm barrels and had the items shipped to the Subject Premises. As described in further detail below, on or about November 8, 2022, BETUNI shipped a parcel which contained two similar 7.5 inch AR-15, 5.56 caliber rifle barrels.

30. According to DHL records, a DHL parcel bearing tracking number 2256433244 ("Subject Parcel 1") was dropped off at a pack and ship business ("Business 1") located in Bridgeview, Illinois on or about November 8, 2022.

31. According to Employee A at Business 1, he/she identified a driver's license photo of Amin BETUNI as the person who dropped off Subject Parcel 1 on November 8, 2022.

32. Furthermore, Employee A showed me surveillance footage from Business 1 on November 8, 2022. The surveillance footage showed an individual who looked like Amin BETUNI[1] walk into Business 1 with a young child and place a

[1] Based on a comparison to a driver's license photo of Amin BETUNI.

George Foreman Grill box on the front counter and watch as Employee A boxed and taped up the package for shipping.

33. According to documents produced by Business 1, Subject Parcel 1 was paid for using a Visa Credit Card ending in 9446 and in the name of Amin BETUNI. According to Employee A and the receipt, Amin BETUNI spent $380[2] to ship a George Foreman Grill sent to Israel.[3]

34. According to the shipping label, Subject Parcel 1 weighed approximately 10.9 pounds and was declared as a "toaster" with a value of $30.00.

35. According to the shipping label, Subject Parcel 1 was sent from "Ameen BETUNI, 10340 S 73rd Ave, Palos Hills, IL 60465,"[4] Subject Phone 1, and was addressed to "Moneer BETULI, Al Alam Street NO 2, DHL Office Shufat, Jerusalem, Israel 9730000 0528925823".

36. According to records maintained by CBP, on about November 8, 2022, CBP received Subject Parcel 1 for inspection. Pursuant to border search authority,

---

[2] According to an open-source search of the internet, this model of George Forearm Grill is available for $33.58 at WalMart.com. *See* https://www.walmart.com/ip/George-Foreman-4-Serving-Removable-Plate-Grill-and-Panini-Black-GRP1065B/864582486
Last visited February 16, 2023.

[3] According to documents produced by Business 1, Amin BETUNI has sent approximately four prior shipments to Jerusalem, Israel, three of the shipments listed recipient contact phone number 0586326614. Two shipments sent on March 22, 2019, one on April 4, 2019 and another on August 16, 2021. The contents of these parcels were declared by BETUNI as "Engine Freeze Plug", "Electric Exhaust Remot" and "Freeze Plug", and "Electrice Exhaust Remote".

[4] This address is a vacant lot next to the property, which according to the Cook County Assessor's Office, owned by Amin BETUNI.

Subject Parcel 1 was x-rayed by CBP. According to CBP, the x-ray showed two long blacked out areas that obstructed the x-ray image. Subject Parcel 1 was then opened and inspected by hand. During the inspection, CBP Officers discovered that Subject Parcel 1 was a George Foreman grill with two 5.56 caliber, 7.5 inch rifle barrels wrapped in tinfoil and metal slag and secreted within the grill. The rile barrels appeared to be similar to the rifle barrels BETUNI ordered using **Subject Microsoft Account 1**. CBP Officers also located an Apple AirTag[5] device bearing serial number HGMJDCLFP0GV within the shipment.

The Apple AirTag located in Subject Parcel 1 was paired with Subject Apple Account 1

37. According to Apple records, AirTag device bearing serial number HGMJDCLFP0GV was part of a four pack of AirTags sold on September 12, 2022, to Amazon for resale. According to Amazon records, BETUNI purchased a four pack of AirTags on November 7, 2022.

38. Further, according to Apple records, AirTag device bearing serial number HGMJDCLFP0GV was paired with **Subject Apple Account 1** and the device was unpaired with **Subject Apple Account 1** on or about December 21, 2022,

[5] According to Apple's website, an AirTag is a tracking device that sends out the AirTag device's location via a secure Bluetooth signal to an established iCloud account, like Subject Apple Account 1. The user of the iCloud account can see the AirTag's location on a map and monitor the AirTag's location via the Apple Find My app. According to Apple's website, an iCloud account enables users to store and sync data across devices, including Apple AirTag, Apple Mail, backups, files, and tack assets through the Find My app. According to Apple's website, AirTags cannot be shared by multiple accounts and can only be tracked by the paired iCloud account.

at 6:15 a.m. As described in further detail below, BETUNI was not present at the time law enforcement executed search warrant 22M1016 on BETNUI's residence on December 21, 2022. However, law enforcement noticed several web-based security cameras at BETUNI's residence and only ten minutes after law enforcement entered BETUNI's residence, AirTag device bearing serial number HGMJDCLFP0GV was unpaired with **Subject Apple Account 1**.

Subject Microsoft Account 1 ordered additional rifle parts from Online Gun Supply Company 1

39. According to Online Gun Supply Company 1, on or about November 11, 2022, **Subject Microsoft Account 1** ordered four bolt carrier groups[6]. The order was placed by "Chicago Company" to be shipped to the Subject Premises and provided Subject Phone 1 and **Subject Microsoft Account 1** as the contact information. In addition, according to Verizon records, between November 14, 2022, and November 17, 2022, BETUNI's phone, Subject Phone 1, contacted Online Gun Supply Company 1 four times.

40. According to Israeli Customs officials, on or about December 12, 2022, Israeli Customs officials inspected and seized FedEx shipment number 3913 4570 0587 with a listed return address of "Chicago Global Inc." at the Subject Premises and contact number of Subject Phone 1. According to Israeli Customs officials, the

[6] Through my training and experience, I am aware that a bolt carrier group is the part of the rifle that is responsible for performing semiautomatic fire when the trigger is pulled.

shipment was found to contain four bolt carrier groups that were concealed inside a George Foreman Grill as well as an Apple AirTag.

41. Based on law enforcement's comparison, the four bolt carrier groups seized from packages with return labels to BETUNI's residence were similar to the four bolt carrier groups purchased via **Subject Microsoft Account 1** from Online Gun Supply Company 1 approximately one month prior.

Subject Microsoft Account 1 used to order rifle parts from Online Gun Supply Company 2

42. According to Verizon records, on or about October 25 and 26, 2022, Subject Phone 1 was in contact with phone number 828-313-0200, an online seller of various firearms parts ("Online Gun Supply Company 2").

43. According to records maintained by Online Gun Supply Company 2, two days later, October 28, 2022, **Subject Microsoft Account 1** placed an order for rifle parts to be shipped to Amin BETUNI at the Subject Premises. Payment for this order was the same credit card provided to Business 1 as payment for the Subject Parcel 1 on November 8, 2022.

44. According to Online Gun Supply Company 2, the shipment was sent to the Subject Premises on October 28, 2022 and contained an "AR15/M16 Complete Lower Receiver[7] Replacement Parts Set" valued at $179.99. Through my training

[7] Through my training and experience I am aware that a lower receiver replacement parts set can be used in the build of a lower half of a rifle.

and experience I am aware that an "AR15" and "M16" are rifle models. According to Online Gun Supply Company 2's website, the set contained the following parts:

- M16 Trigger
- M16 Hammer
- M16 Disconnector
- M16 GI Sear
- M16 GI Sear Pin
- M16 Selector
- Hammer Pin
- Trigger Pin
- Hammer Spring
- Trigger Guard (Aluminum)
- Trigger Guard Roll Pin
- Bolt Catch
- Bolt Catch Detent
- Bolt Catch Detent Spring
- Bolt Catch Roll Pin
- Buffer Detent
- Buffer Detent Spring
- Trigger Spring
- Disconnector Spring
- Mag Catch
- Mag Catch Spring
- Mag Catch Button
- Selector Detent
- Selector Detent Spring
- Pivot Pin
- Pivot Pin Detent
- Pivot Pin Detent Spring
- Takedown Pin
- Takedown Pin Detent
- Takedown Pin Detent Spring
- A2 Grip
- Grip Screw
- Star Washer

45. According to Employee B at Online Gun Supply Company 2, on November 8, 2022, an email from Online Gun Supply Company 2 containing an invoice of the purchase made by BETUNI was sent to **Subject Microsoft Account 1**. The invoice stated: "Firearms parts are controlled under Export Administration

Regulations (EAR) as well as International Traffic in Arms Regulations (ITAR); and may not be exported without proper authorization by the U.S. Department of Commerce and/or U.S. Department of State."

46. According to United States Postal records, on or about October 28, 2022, a shipment originating from Online Gun Supply Company 2 shipped to: Amin BETUNI at the Subject Premises.

Subject Google Account 1 was used to order rifle parts from Online Gun Supply Company 3

47. According to Online Gun Supply Company 3, on or about November 15, 2022, BETUNI, using **Subject Google Account 1**, purchased ten AR-15 gas blocks[8] and had the items shipped to the Subject Premises.

48. According to an HSI Special Agent assigned to the embassy located in Tel Aviv, Israel, on or about December 8, 2022, Israeli Customs officials inspected and seized FedEx shipment number 3909 1548 2440 with a listed return address of Amin BETUNI at the Subject Premises and contact number of Subject Phone 1. According to Israeli Customs officials, the shipment was found to contain at least six gas blocks for rifles that were concealed inside of auto parts.

49. Also located in the shipment was a concealed Apple AirTag. The shipment was addressed to "Muneer Betuli, Al Alam Street #2, Jerusalem".

[8] Through my training and experience, I am aware that a gas block acts as a connector for the barrel and the gas tube on a rifle, which holds the tube in place and channels the gas back toward the bolt carrier group.

According to Israeli Customs officials, the contents of the parcel were declared as "Auto parts-car parts". The recipient's name and address on this shipment appears to be very similar to that of the Subject Parcel 1.

Other shipments sent to Israel from BETUNI

50. According to Israeli Customs officials, other shipments listing BETUNI as the sender with a return address of the Subject Premises have been delivered to individuals in Israel in the past. For example, on or about November 1, 2022, BETUNI, listing the Subject Premises as the return address, sent FedEx shipment number 3901 0567 9685 to an individual named Umsameer BETINI located at Aqsa Express, Al Alam St #2, Jerusalem, Israel. The contents of the parcel were declared as "Appliances – (2) Electric Grills". According to the FedEx website, this parcel was delivered on November 8, 2022. According to Verizon records, Subject Phone 1 had contact with a FedEx tracking system number approximately seven times between November 6, 2022, and November 8, 2022. Additionally, on or about November 12, 2022, BETUNI, listing the Subject Premises as the return address, sent FedEx shipment number 3905 5751 0324 to an individual named Muneer BETULI located at Al Alam Street Number 2, Jerusalem, Israel. The contents of the parcel were declared as "Automotive Parts-1 Honda Alternator". According to Google records, **Subject Google Account 1** communicated with notificaitions@fedex.com between November 15, 2022, and November 29, 2022. According to publicly available FedEx records, this parcel was delivered on November 20, 2022.

51. On or about November 18, 2022, BETUNI, listing the Subject Premises as the return address, sent FedEx shipment 3908 3693 1643 to an individual named Muneer BETULI located at Al Alam Street Number 2, Jerusalem, Israel, with contact phone number 0586326614. The contents of the parcel were declared as "Gift Shipment – 1 grill and 1 sandwich grill". According to publicly available FedEx records, this parcel was delivered on November 24, 2022. Additionally, according to Verizon records, Subject Phone 1, had contact with the listed recipient phone number days before and subsequent to the shipping date. According to Google records, **Subject Google Account 1** communicated with fedex@message.fedex.com approximately seven times from November 13, 2022, through December 7, 2022.

Subject Google Account 2 was used to order rifle parts from Online Gun Supply Company 4

52. According to Online Gun Supply Company 4, on or about November 29, 2022, an individual purporting to be "Johnny Duda" using **Subject Google Account 2** made an online order for an AR-15 gas block. The order was shipped to the Subject Premises and listed Subject Phone 1 as the contact phone number. As described below, on December 21, 2022, law enforcement executed a search warrant on the subject premises and recovered a gas block inside of an envelope addressed to "Johnny Duda" at the Subject Premises.

Search warrant executed at the Subject Premises

53. On December 21, 2022, law enforcement executed a search warrant[9] at the Subject Premises. BETUNI was not present at the time of the search. Law enforcement located three Glock switches (machineguns)[10] concealed inside of a band-aid box located in the same closet that BETUNI's wife stated contained BETUNI's items along with several extended drum magazines for a 9mm firearm as well as an AR style rifle. Located in the same closet, law enforcement located a Glock 26 9mm pistol, an AR-15 style rifle, a shotgun and $20,000 in cash.

54. Law enforcement also located what appeared to be a packaged bolt carrier group inside of a closet that BETUNI's wife identified as BETUNI's closet.

55. Law enforcement also located one suspected silencer[11] in the garage of the Subject Premises that fit onto the AR-15 rifle located in BETUNI's closet. This silencer did not appear to have any serial numbers affixed to it.

---

[9] 22 M 1016

[10] The National Firearms Act (NFA), 26 U.S.C.§5845(b), defines "machinegun" as "any weapon which shoots, is designed to shoot, or can be readily restored to shoot, automatically more than one shot, without manual reloading, by a single function of the trigger. The term shall also include the frame or receiver of any such weapon, any part designed and intended solely and exclusively, or combination of parts designed and intended for use in converting a weapon into a machinegun, and any combination of parts from which a machinegun can be assembled if such parts are in the possession or under the control of a person."

[11] Title 18 U.S.C. § 921(a)(24), defines "firearm silencer" as "any device for silencing, muffling, or diminishing the report of a portable firearm. Including any combination of parts, designed or redesigned, and intended for use in assembling or fabricating a firearm silencer or firearm muffler, and any part intended only for use in such assembly or fabrication."

Consent Search of BETUNI's wife's cellular telephone

56. During the execution of the search warrant at the Subject Premises, investigating agents received verbal and written consent to search the cellular telephone belonging to BETUNI's wife.

57. During a search of the wife's cellular telephone, agents located WhatsApp text messages between BETUNI and his wife relating to firearms parts. For example, a WhatsApp text string between BETUNI, using Subject Phone 1, and his wife showed photographs of rifle bolt carrier groups that BETUNI's wife stated had recently been received in the mail at the Subject Premises. According to the HSI agent in Tel-Aviv, Israel, these bolt carrier groups looked like the bolt carrier groups that had been recently seized by Israeli Customs personnel.

BETUNI's cellular telephone re-set to factory mode

58. On or about December 22, 2022, law enforcement informed BETUNI that they had a search warrant for Subject Phone 1.[12] BETUNI agreed to meet law enforcement at a Starbucks in Chicago Ridge, Illinois, and handed over Subject Phone 1, an Apple iPhone, which he said was his work phone.

59. According to an HSI Computer Forensics Analyst, the phone BETUNI gave law enforcement was an Apple iPhone assigned the same telephone number as Subject Phone 1 but the phone had been reset to factory default. According to the

[12] 22 M 1017

HSI Computer Forensics Analyst, resetting a phone to factory default erases all data previously stored on the device. As a result of the factory reset, no data was recovered from Subject Phone 1.

License Determinations

60. On or about December 8, 2022, a Department of Commerce Special Agent reviewed License Determination E1075726 from a Bureau of Industry and Security Licensing Officer. Per the officer, the barrels for the 5.56 M4 Style rifles found secreted in Subject Parcel 1 seized by CBP on November 18, 2022, are assigned Export Classification Control number 0A501.c and require a license from BIS to be exported to Israel. The officer also advised that a "Limited Value Shipment" license exception may apply if the item is valued under $500.

61. According to 15 CFR § 740, which governs Bureau of Industry and Security License exceptions, section 1(b) states that "by using any of the license exceptions, you are certifying that the terms, provisions, and conditions for the use of the License Exception described in the EAR have been met. Please refer to part 758 of the EAR for clearance of shipments and documenting the use of License Exceptions."

62. In addition, 15 CFR § 758, which governs export clearance requirements and authorities, states in section 1(d) "… When an exemption from filing the Electronic Export Information applies, the export authority (license exception or no license required) must be entered on the loading document (e.g Cargo Declaration,

manifest, bill of lading, (master) air waybill) by the person responsible for preparing the document."

63. According to the Automatic Export System, a U.S. government database which contains information on exports from the United States, called Electronic Export Information. The system contained no results for any shipments from Amin BETUNI. Further, a review of the DHL Airway bill for Subject Parcel 1 contained no annotation of a BIS license exception of any type.

64. Based on my training and experience in other investigations, I believe that a search of electronic account contents of individuals engaged in criminal conduct yields investigative evidence and leads relating to:

a. the identities of participants engaged in and witnesses to the **Subject Offenses**;

b. the contact information of participants engaged in and witnesses to the **Subject Offenses**;

c. the timing of communications among participants and other individuals involved in the **Subject Offenses**;

d. the methods and techniques used in the **Subject Offenses**;

e. information regarding the physical location of participants engaged in and witnesses to the **Subject Offenses**; and

f. additional transactions involving smuggling goods from the United States.

III. SEARCH PROCEDURE

65. In order to facilitate seizure by law enforcement of the records and information described in Attachment A, this affidavit and application for search warrant seek authorization, pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to permit employees of the **Service Providers** to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented:

66. The search warrant will be presented to the **Service Provider's** employees who will be directed to the information described in Section II of Attachment A;

67. In order to minimize any disruption of computer service to innocent third parties, the **Service Provider's** employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II of Attachment A, including an exact duplicate of all information stored in the computer accounts and files described therein;

68. The **Service Provider's** employees will provide the exact duplicate in electronic form of the information described in Section II of the Attachment A and all information stored in those accounts and files to the agent who serves this search warrant; and

69. Following the protocol set out in the Addendum to Attachment A, law enforcement personnel will thereafter review all information and records received

from the **Service Provider's** employees to locate the information to be seized by law enforcement personnel pursuant to Section III of Attachment A.

IV. CONCLUSION

70. Based on the above information, I respectfully submit that there is probable cause to believe that evidence violations of Title 50, United States Code, Section 1705, Title 18, United States Code, Section 1343, and Title 13, United States Code, Section 305 are located within one or more computers and/or servers found at Apple Inc. that accepts service at One Apple Park Way, Cupertino, CA 95014; Google LLC, located at 1600 Amphitheatre Parkway, Mountain View, California, 94043; and Microsoft Corporation located at One Microsoft Way, Redmond, WA 98052-6399. By this affidavit and application, I request that the Court issue a search warrant directed to Apple Inc., Google LLC, and Microsoft Corporation allowing agents to seize the electronic evidence and other information stored on the Apple Inc., Google LLC, and Microsoft Corporation servers following the search procedure described in Attachment A and the Addendum to Attachment A.

FURTHER AFFIANT SAYETH NOT.

Daniel Nugent
Special Agent
Homeland Security Investigations

Sworn to and affirmed by telephone 21st day of February, 2023

Honorable GABRIEL A. FUENTES
United States Magistrate Judge

ATTACHMENT A

I. SEARCH PROCEDURE

1. The search warrant will be presented to Apple Inc.'s personnel, who will be directed to isolate those accounts and files described in Section II below.

2. In order to minimize any disruption of computer service to innocent third parties, company employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein.

3. Apple Inc.'s employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant. Provider shall disclose responsive data, if any, by sending to Special Agent Daniel Nugent, 747 E. 22nd Street, Suite 3000, Lombard, Illinois 60148, Daniel.B.Nugent@ice.dhs.gov, using the US Postal Service or another courier service, notwithstanding 18 U.S.C. § 2252A or similar statute or code.

4. Following the protocol set out in the Addendum to this Attachment, law enforcement personnel will thereafter review information and records received from company employees to locate the information to be seized by law enforcement personnel specified in Section III below.

II. FILES AND ACCOUNTS TO BE COPIED BY EMPLOYEES OF

To the extent that the information described below in Section III is within the possession, custody, or control of Apple Inc., which are stored at premises owned, maintained, controlled, or operated by Apple Inc., which are stored at One Apple Park Way, Cupertino, CA 95014, Apple Inc., is required to disclose the following information to the government for the following account:

aminbetuni@icloud.com

Records to be disclosed by Apple Inc.

a. The contents of all communications and related transactional records for all Provider services used by an Account subscriber/user, including but not limited to incoming, outgoing, and draft e-mails, messages, calls, chats, and other electronic communications; attachments to communications (including native files); source and destination addresses and header or routing information for each communication (including originating IP addresses of e-mails); the date, size, and length of each communication; and any user or device identifiers linked to each communication (including cookies);

b. The contents of all data related transactional records for all Provider services used by an Account user (including by not limited to e-mail services, calendar services, file sharing or storage services, photo sharing or storage services, remote computing services, content or remotely accessed data and servers connected to subject domains and subject IP addresses that is accessible through Provider's

services, instant messaging or chat services, and voice call services); including any information generated, modified, accessed, or stored by user(s) or Provider in connection with the Account (such as contacts, calendar data, images, videos, notes, documents, bookmarks, profiles, device backups, any saved passwords, and any other saved or accessible information);

c. All Provider records concerning the online search and browsing history associated with the Account or its users (such as information collected through tracking cookies);

d. All records and other information concerning any document, or other computer file created, stored, revised, or accessed in connection with the Account or by an Account user, including the contents and revision history of each document or other computer file, and all records and other information about each connection made to or from such document or other computer file, including the date, time, length, and method of connection; server log records; data transfer volume; and source and destination IP addresses and port numbers;

e. All records regarding identification of the Account, including names, addresses, telephone numbers, alternative e-mail addresses provided during registration, means and source of payment (including any credit card or bank account number), records of session times and durations (including IP addresses, cookies, device information, and other identifiers linked to those sessions), records of account registration (including the IP address, cookies, device information, and other

identifiers linked to account registration), length of service and types of services utilized, account status, methods of connecting, all passwords, and server log files;

f. All device or user identifiers which have ever been linked to the Account, including but not limited to all cookies and similar technologies, unique application numbers, hardware models, operating system versions, device serial numbers, Global Unique Identifiers ("GUID"), mobile network information, telephone numbers, Media Access Control ("MAC") addresses, and International Mobile Equipment Identities ("IMEI");

g. Basic subscriber records and login history (including, as described in 18 U.S.C. § 2703(c)(2), names, addresses, records of session times and durations, length of service and types of service utilized, instrument numbers or other subscriber numbers or identities, and payment and password information) concerning any Provider account (including both current and historical accounts) ever linked to the Account by a common e-mail address (such as a common recovery e-mail address), or a common telephone number, means of payment (*e.g.*, credit card number), registration or login IP addresses (during one-week period), registration or login cookies or similar technologies, or any other unique device or user identifier;

h. All records of communications between Provider and any person regarding the Account, including contacts with support services and records of actions taken;

i. Information about any complaint, alert, or other indication of malware, fraud, or terms of service violation related to the Account or associated user(s), including any memoranda, correspondence, investigation files, or records of meetings or discussions about the Account or associated user(s) (but not including confidential communications with legal counsel); and

j. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

Pursuant to 18 U.S.C. § 2703(d), the service provider is hereby ordered to disclose the above information to the government within 14 days of the signing of this warrant.

III. Information to be Seized by Law Enforcement Personnel

All information described above in Section II that constitutes evidence and instrumentalities concerning violations of Title 18, United States Code, Section 554, Title 50, United States Code, Section 4819 and Title 18, United States Code, Section 922(o), as follows:

1. Items related to the identity of the user or users of the **Subject Accounts**.

2. Items related to the physical location of the users of the **Subject Accounts** at or near the times of the **Subject Offenses**.

3. Items related to the export of any products from the United States or from any United States company, or involving any United States person to any other

country or the shipment or transshipment of any products from one country to another:

4. Items related to firearms purchases, sales, construction, or rebuilding.

5. Items regarding the identity of any co-conspirators;

6. Contracts, invoices, purchase orders, payment information, and shipping instructions and documentation related to U.S. origin goods, any goods which may be otherwise controlled, and the corresponding information.

7. Items related to who created the Subject Accounts, and any associated accounts, including records about their identities and whereabouts;

8. All non-content information described about in Section II.

ADDENDUM TO ATTACHMENT A

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant requires the recipient of the warrant to copy and produce the contents of an electronic account so that they may be reviewed in a secure environment for information consistent with the warrant.

The account provider shall provide the government only data that fall within the criteria as described in Attachment A(I), which may either be the entire contents of an account or only a subset of an account.

The government's review of the data shall be conducted pursuant to the following protocol:

The government must make reasonable efforts to use methods and procedures that will locate only those categories of data, files, documents, or other electronically stored information that are identified in the warrant, while minimizing exposure or examination of categories that will not reveal the items to be seized in Attachment A(III).

The review of electronically stored information contained in the account described in Attachment A may include the below techniques. These techniques are a non-exclusive list, and the government may use other procedures that minimize the review of information not within the list of items to be seized as set forth in Attachment A(III):

a. examination of categories of data contained in the account to determine whether that data falls within the items to be seized as set forth in Attachment A(III);

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment A(III);

c surveying various file directories and folders to determine whether they include data falling within the list of items to be seized as set forth in Attachment A(III);

d. opening or reading portions of files, and performing key word or concept searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment A (III); and

e. using forensic tools to locate data falling within the list of items to be seized as set forth in Attachment A(III).

Law enforcement personnel are not authorized to conduct additional searches for any information beyond the scope of the items to be seized by this warrant as set forth in Attachment A(III). To the extent that materials produced by the account provider pursuant to this search warrant contain evidence of crimes not within the scope of this warrant appears in plain view during the government's review, the government shall submit a new search warrant application seeking authority to expand the scope of the search prior to searching portions of that data or other item that is not within the scope of the warrant. However, the government may continue its search of that same data or other item if it also contains evidence of crimes within the scope of this warrant.